chinaXiv:201810.00031v1

基于激活标志位的改进 RFID 密钥无线生成算法 *

杨　俊[1]，邹志革[2]

(1. 武汉职业技术学院, 武汉 430074; 2. 华中科技大学, 武汉 430074)

摘　要：针对现有三种常见无线射频识别密钥无线生成场景下，设计的相应密钥生成算法中存在的算法理论证明缺失、重放攻击、密钥伪造攻击以及 RFID 标签身份 ID 泄露的安全性问题，设计了更安全的基于激活标志位的改进 RFID 系统密钥无线生成算法。改进算法仅基于多种超轻量级位运算来组合构建安全的算法框架，降低成本，提高效率；利用激活标志位 AckBit 机制以及新鲜性机制抵抗重放、密钥伪造攻击；通过完整 GNY 逻辑证明过程与安全性对比分析，证明目标算法的安全可行性。最后，给出原算法与改进算法之间的标签成本代价对比，表明改进的算法在满足低成本的条件下具有更高的安全性。

关键词：无线射频识别；密钥无线生成；更安全；激活标志位；GNY 逻辑证明

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2018.06.0404

Improved RFID key wireless generation algorithm based on activation flag

Yang Jun[1], Zou Zhige[2]

(1. *Wuhan Polytechnic*, *Wuhan* 430074, *China*; 2. *Huazhong University of Science & Technology*, *Wuhan* 430074, *China*)

Abstract: In the scenario of wireless generation of three common radio frequency identification keys, the security key problem of replay attack, key forgery attack and RFID tag identity ID leakage and the lack of algorithm theory are found in the corresponding key generation algorithms. This paper designed a more secure RFID-based key generation algorithm based on activation flag. The improved algorithm only combined multiple super-lightweight bit operations to construct a secure algorithm framework, which reduced cost and improves efficiency. It used the activation flag 'AckBit' mechanism and the freshness mechanism to resist replay and key forgery attacks. Through the complete GNY logic proof process and safety comparison analysis, it proved the safety and feasibility of the target algorithm. Finally, This paper presented the comparison of the tag cost between the original algorithm and the improved algorithm, which shows that the improved algorithm has higher security under the condition of satisfying the low cost.

Key words: RFID; wireless key generation; more secure; activation flag; GNY logic proof

0　引言

随着物联网的不断发展其感知层的重要技术——无线射频识(radio frequency identification，RFID)也越来越受到人们的重视[1]。在 RFID 系统中标签和读写器通常需要进行相互认证、识别、定位等操作，这就需要共享密钥的参与，而密钥的下发通常有两种方式一种是在出厂已经设置好，密钥值单一固定；另一种方式是通过密码学相关算法手段在读写器和标签两端同时实现密钥的无线生成，具有动态、便捷的优点[2-3]。这第二种方法是近年来的研究热点，但是也正是由于 RFID 系统这种动态开放性，使得共享密钥如何快速、安全、准确的生成成为了当下 RFID 密钥无线生成算法需要解决的重点问题[4]。近年来以超轻量位运算为基础的密钥无线生成算法，因为其具有动态不可预测性、成本低、安全性较为可靠等优点被广泛研究。

1　相关研究

文献[5]首次提出 RFID 密钥无线生成思想，跳出了密钥事先预设带来的局限性，并根据“后向信道不可窃听”的假设，提出了“WiKey” RFID 密钥无线生成算法。但是，随后多篇文献指出了 WiKey 算法假设的应用局限性，大多指出了其因为所有通信数据均明文传输而存在密钥伪造的风险，并分别提出了各自的改进算法，主要有文献[6-9]，其中主要优缺点具体分析如下：

文献[6]提出了一种基于多种位运算（字合成位运算、交叉位运算、异或、与运算）的 RFID 密钥生成算法。其利用标签编号信息通信，认证效率有所提升，但是该算法在单标签密钥

收稿日期：2018-06-26；**修回日期：**2018-07-31　**基金项目：**湖北省教育厅科学技术研究计划指导性项目（B201658）

作者简介：杨俊（1975-），男，湖北武人，副教授，主要研究方向为通信技术、信息处理及人工智能；邹志革（1975-），男，湖北宜昌人，副教授，博士，主要研究方向为集成电路设计与应用、嵌入式系统设计.

ChinaXiv合作期刊

生成场景中其实也存在标签身份 ID 暴露的风险；又因为系统标签端每个标签都需要生成随机数来进行认证计算，这会增加系统成本与复杂性，不能满足低成本应用。

文献[7]也提出了一种新的密钥生成算法，虽然解决了 WiKey 算法的安全性缺陷，但是该算法的认证过程需要进行两轮通信才能完成，效率不高。

文献[8]提出了一种基于标签部分 ID 的改进算法，该算法由于只引入标签 ID 信息和随机数，成本较低，适合低成本应用环境，但是通过本文的研究发现该算法在生成群组标签的场景下，因为不能抵抗窃听、重放攻击而造成标签身份泄露以及密钥伪造。具体漏洞分析如下：①标签身份泄露漏洞：因为在通信过程中，攻击者 A 可以窃听第二步通信过程，组内标签 T_i 会发送 $M_i=ID_{ir}\oplus ID_{il}$ 得到所有标签的 M_i，接着继续窃听第三步，读写器向所有标签明文发送 (ID_{il},k_i)，攻击者 A 即可根据窃听得到的信息，解密得到 $ID_{ir}=M_i\oplus ID_{il}$，因为事先已经获得窃听得到的明文标签 ID 的左半部分，这样标签完整身份 ID 信息得到（$ID_i=ID_{il}\parallel ID_{ir}$），标签身份泄露。②密钥伪造漏洞：又因为算法设计中缺少随机数新鲜性验证，攻击者 A 完全可以假冒标签，重放 M_i 或者根据解密得到的 (ID_{ir},ID_{il}) 重新计算 M_i，通过数据库的合法性验证得到密钥计算因子 k_i，解密得到密钥 $k=k_i\oplus ID_{ir}$，或者直接根据已经得到的所有标签 ID 信息，直接计算得到密钥 k。因此，该算法不能抵抗重放攻击存在密钥伪造以及标签身份泄露风险。

文献[9]提出了一种基于假名标志的加密 RFID 密钥生成算法，引入假名标志一定程度上可以防止标签身份信息泄露，但是经过本文的研究发现，该算法在单个标签密钥生成场景下仍然存在密钥伪造攻击漏洞。因为，在读写器向标签发送加密的 $A=r_1\oplus IDS$、$B=r_2\oplus IDS$ 消息时，攻击者可以直接通过窃听跟踪得到消息 A、B，并用这两个数据本身破解计算（$A\oplus B=r_1\oplus IDS\oplus r_2\oplus IDS=r_1\oplus r_2=k$）即可得到该算法的密钥信息 k，所以攻击者可以根据算法本身设计的漏洞快速暴力破解得到系统密钥信息 k，因此该协议存在密钥伪造攻击漏洞。

综上所示，现有的 RFID 系统密钥无线生成算法主要存在以下缺点，如表 1 所示。

表 1　现有算法漏洞分类

现存协议缺点	相关文献
效率较低	文献[7]
缺少形式化证明	文献[5、6、7、8、10]
重放攻击	文献[5、8、9]
标签身份 ID 泄露	文献[6、8]
密钥伪造攻击	文献[5、6、8、9、10]

针对以上文献[5]和文献[8，9]中存在的算法漏洞，本文提出了一种改进的更安全的在单标签密钥生成、多标签密钥生成、群组标签密钥生成三种场景下分别适用的算法。

2　改进的更安全的 RFID 系统密钥无线生成算法

2.1　前提与符号说明

同一般 RFID 系统密钥无线生成算法的基本前提假设特征相似，后台数据库和读写器之间视为统一安全整体，下文统称读写器；而读写器和标签之间视为不安全的通信信道[11-12]因此需要在设计协议时进行加密传输保证安全性。其中自组合交叉位运算 *Sac(X,Y)*基本原理参考文献[13]，本算法所需符号说明如下表 2 所示。

表 2　符号说明

符号	含义
Tag	合法标签
Reader	合法读写器
ID	标签唯一身份标志、
TID	标签假名身份标志
TID_L	标签假名身份标志的左部分
TID_R	标签假名身份标志的右部分
Key	标签与读写器之间共享密钥
k_i	密钥生成因子
AckBit	激活标志位, *AckBit=1* 标签激活；*AckBit=0* 标签未激活
r_1、r_2	标签与读写器之间随机数
r_l、r_r	随机数的左、右两部分
A，B，C，D	通信数据
Sac(X,Y)	自组合交叉位运算
Rot(X,Y)	循环移位运算
$\oplus$	异或运算

2.2　算法具体过程

在协议初始状态中，标签保存唯一身份标志 *ID*,，并且利用自身的标志信息 *ID* 生成标签 *Tag* 的假名信息 $TID=Rot(ID_L,ID_R)$，将 *TID* 的左右两部分保存，最后标签端存储字段内容为 (ID_i,TID_i_L,TID_i_R)，其中 i 为标签标号；每个标签在读写器中的数据存储结构为(*i*，*ID*，TID_i_L，TID_i_R，*AckBit=0*（初始状态为 0）)。

2.2.1 基于多标签密钥批量无线生成场景下算法

读写器为多标签批量生成相应的个体密钥算法具体过程如下，如图 2 所示。多密钥生成与单密钥生成算法过程相似，不同之处在于：

a）Tag_1，…，*Tag*i 多个标签发送密钥生成请求命令以及自身标号 i，<*Rq*，1，4，*i*，…>等待读写器回复。

b）读写器在给定时间内内依次响应并按标号 *i* 顺序排队等待验证，所有标签 T_i，依次按步骤 c)~f)完成密钥的生成过程，如果超时或者认证失败，协议终止；如果数据库同步生成密钥成功后，进行步骤 f)。

c）读写器根据标签发送的标号 *i* 以及激活标志 *AckBit* 判断算法是否继续。如果检索到 *i* 并且激活标志 *AckBit*=0，算法继续，将检索到的数据(*i*，ID_i，TID_i_L，TID_i_R，*AckBit*)计算得到

chinaXiv:201810.00031v1

chinaXiv:201810.00031v1

对应的 $TID_i = Rot(ID_i_L, ID_i_R)$，并生成两个随机数 r_1、r_2，计算得到 $A=TID_i_L \oplus r_1$、$B=TID_i_R \oplus r_2$，最后将 A、B 发送给标签 *Tag*；如果标号 i 检索成功但是激活标志 *AckBit=1*，说明标签密钥已生成过，重复申请，算法终止；如果标号 i 检索失败，算法终止。

d）标签 *Tag* 在收到数据 A、B 后，利用事先存储的假名信息 (TID_i_L, TID_i_R)，解密 A、B 得到随机数 r_1、r_2，具体解密过程如下：$r_1=TID_i_L \oplus A$、$r_2=TID_i_R \oplus B$，解密成功后，标签生成待验证数据 C，$C = Rot(r_1_L, TID_i_L) \oplus Rot(r_2_L, TID_i_L)$，最后将数据 C 发送给读写器。

e）读写器收到消息 C 后，通过原有生成的 r_1、r_2 以及 TID_i 信息，计算得到 C'，随后验证 C 是否等于 C'，如果相等读写器验证标签成功，标签合法，向标签发送密钥生成命令 *Create*，同时数据库同步为标签生成密钥 Key_i，$Key_i = Sac(r_1_R, ID_i) \oplus Sac(r_2_R, ID_i)$，得到标签新的存储字段(i，*ID*，$TID_i_L$，$TID_i_R$，$Key_i$，*AckBit*=1)。

f）标签 *Tag* 收到密钥生成命令 *Create* 后，密钥生成得到 Key_i，$Key_i = Sac(r_1_R, ID_i) \oplus Sac(r_2_R, ID_i)$。

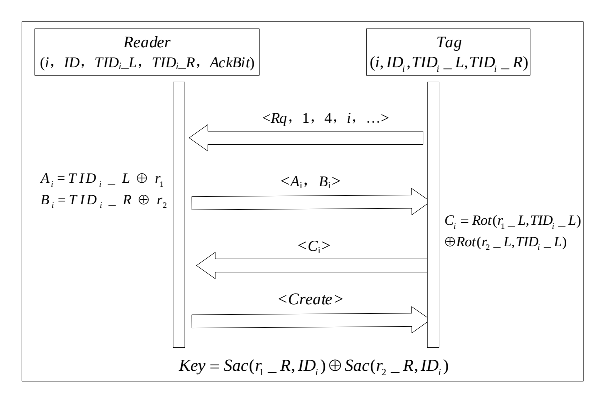


图 1　基于多标签密钥批量无线生成场景下改进算法过程图

2.2.2 基于单标签密钥无线生成场景下算法

读写器为单个标签生成相应的个体密钥算法作为多标签的特例具体过程将不做重复描述，单标签过程图具体如下，如图 2 所示。

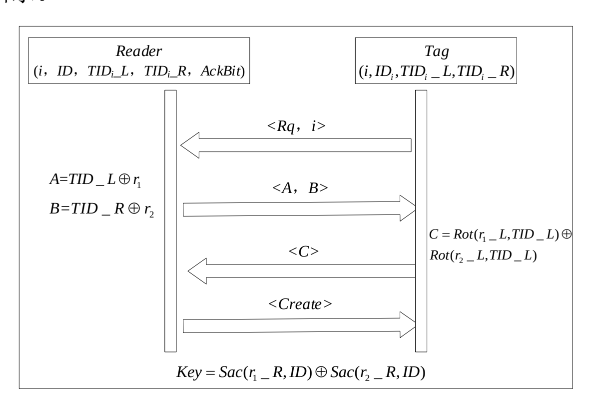


图 2 基于单标签密钥无线生成场景下改进算法过程图

2.2.3 基于组标签组密钥无线生成场景下算法

读写器为群组标签生成统一的组密钥算法具体过程如下，如图 3 所示。

a）首先读写器向群组标签广播，下发密钥生成命令。

b）群组标签收到命令 Rq 后，组内所有标签分别利用自身的假名信息计算得到验证数据 A_1，A_2，…A_i，并将所有 A_i 信息发送给读写器，$A_i = Rot(TID_i_L, TID_i_R) \oplus i$。

c）读写器收到所有 A_i 信息后，在给定的时间内，根据存储的字段信息(*i*，*ID*，TID_i_L，TID_i_R，*AckBit*)，计算 $A_i \oplus i = Rot(TID_i_L, TID_i_R)$，检查读写器组内标签记录中的字段是否全部有对应的 A_i 消息满足，如果全部满足并且相等，说明组内所有标签的信息在读写器中都可以找到，组内所有标签激活成功，读写器存储的字段信息更新为(*i*，*ID*，TID_i_L，TID_i_R，*AckBit*=1)；若读写器组内标签记录中任意一条记录未与标签发送的 A_i 消息对应，组内标签激活失败，在给定时间内，再次启动新一轮激活，直到组内标签记录全部相等，如果时间超时，算法终止。当组内所有标签激活成功后，读写器生成随机数 r，开始为群组标签生成共享组密钥 *Key*，$Key = Sac(ID_1, r) \oplus Sac(ID_2, r) \oplus \cdots \oplus Sac(ID_i, r)$，并为组内每个标签生成加密的组密钥计算因子 K_i，$K_i = Key \oplus Sac(ID_i, r)$，因为组内标签需要得到随机数 r 才能解密得到组密钥 *Key*，所以读写器还需为组内标签发送一组消息 B_i、C_i、D_i，具体加密过程如下：$B_i = TID_i_L \oplus r_L$，$C_i = TID_i_R \oplus r_R$，$D_i = Rot(TID_i, r)$。最后向标签发送消息<K_i、B_i、C_i、D_i>。

d）组内标签在收到消息<K_i、B_i、C_i、D_i>后，首先根据各标签端存储字段内容为 (ID_i, TID_i_L, TID_i_R)，解密得到随机数 r，具体解密过程如下：$r_L = TID_i_L \oplus B_i$，$r_R = TID_i_R \oplus C_i$，$r = r_L \| r_R$。随后标签计算得到 D'，验证是否和收到 D 相等，如果相等，说明标签对读写器验证成功，组内各标签利用解密得到的 r 以及自身的身份 ID 信息计算得到组密钥 Key_i，$Key_i = K_i \oplus Sac(ID_i, r)$。并依次向读写器发送确认命令 $S_i = Key_i \oplus TID_i_L \oplus TID_i_R$。

e）读写器在规定时间内收到组内所有 S_i 确认命令，需要对比组内标签计算得到的组密钥是否全部相等。Reader 根据存储的各个标签字段(*i*，*ID*，TID_i_L，TID_i_R，*AckBit*=1)，解密 S_i，解密得到如果 $Key_1 = Key_2 = \cdots = Key_i$ 全部相等，说明组内各个标签成功得到组密钥，最后，读写器存储的字段信息更新为(*i*，*ID*，TID_i_L，TID_i_R，*Key*，*AckBit*=1)，向标签组广播回复 update 命令；如果有任意 Key_i 不相等，说明组密钥因子错误，算法终止。

f）标签端收到 update 命令，组内各标签存储字段内容更新为 $(ID_i, TID_i_L, TID_i_R, Key)$，至此算法完成。

综上所述，本节分别在三种不同场景下设计了改进的更安全的的可密钥伪造、标签隐私泄露的 RFID 系统密钥无线生成算法，该算法基于循环移位、异或、自组合交叉位运算实现标签激活和加密认证过程；在组密钥生成场景下引入随机数保证密钥新鲜性，防止重放攻击；在整个通信过程中标签真实身份 ID 匿名隐藏，仅利用假名 TID 代替 ID 进行计算，防止身份泄露；利用标签标号 i 和 *AckBit* 激活标志位的对应关系标记标签

状态信息，提高算法效率。

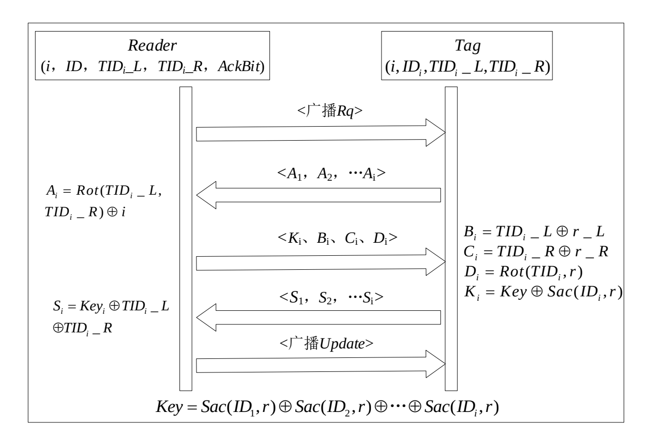


图 3　基于组标签密钥无线生成场景下改进算法过程图

3　算法形式化证明

GNY 逻辑是基于知识和信念的逻辑推理方法之一，其证明思想与方法较普遍的应用在 RFID 算法证明中。GNY 逻辑是由若干公理、规则组成其基本定义可参见文献[14,15]，本文证明过程中主要用到了以下规则：

可识别规则 R_1= $\dfrac{P|\equiv\phi(X)}{P|\equiv\phi(X,Y),P|\equiv\phi(F(X))}$

可识别规则 R_2= $\dfrac{P|\equiv\phi(X),P\in K}{P|\equiv\phi(X)_K,P|\equiv\phi(F(X,K))}$

新鲜性规则 F_1= $\dfrac{P|\equiv\#(X)}{P|\equiv\#(X,Y),P|\equiv\#(F(X))}$

消息解析规则 I_1=

$$\frac{P\lhd *(X)_K,P\in K,P|\equiv P\xleftrightarrow{K}Q,P|\equiv\phi(X),P|\equiv\#(X,K)}{P|\equiv Q|\sim X,P|\equiv Q|\sim(X)_K,P|\equiv Q\in K}$$

1）初始化假设

由于 3 种不同场景算法过程类似，本节只对基于单标签密钥生成改进算法作具体分析证明，其余两种情况由于过程类似，篇幅有限，将不做重复描述。

首先对单个标签密钥生成算法进行初始化假设，其中，H_1、H_2 表示标签、读写器已经拥有的；H_3、H_4 表示标签、读写器相信各自某些信息是可识别的；H_5、H_6 表示标签、读写器对某些数据新鲜性的相信。

H_1：$Tag\in(i,ID,TID_L,TID_R)$

H_2：$Reader\in(i,ID,TID_L,TID_R)$

H_3：$Tag|\equiv\phi(i)$

H_4：$Reader|\equiv\phi(r_1,r_2)$

H_5：$Tag|\equiv\#(r_1,r_2)$

H_6：$Reader|\equiv\#(TID,r_1,r_2)$

2）形式化模型

对单个标签密钥生成算法作过程进行 GNY 逻辑形式化建模，完整模拟算法交互过程。其中，用 M 表示通信过程，标签主体用 Tag 表示，读写器用 Reader 表示。

M_1：$Reader\lhd *(i)$

M_2：$Tag\lhd *F_1(r_1,TID_L),F_2(r_2,TID_R)$

M_3：$Reader\lhd *F_3(r_1_L,r_2_L,TID_L)$

3）安全目标

对单个标签密钥生成算法用 GNY 逻辑语言定义需要达到的安全性目标，其中，D_1 表示读写器对标签身份的初次识别；D_2、D_3 表示标签对读写器验证，对发送信息新鲜性的相信；D_4 表示读写器对标签验证，对标签身份的再次识别。

D_1：$Reader|\equiv Tag|\phi(i)$

D_2：$Tag|\equiv Reader|\sim\#F_1(r_1,TID_L)$

D_3：$Tag|\equiv Reader|\sim\#F_2(r_2,TID_R)$

D_4：$Reader|\equiv Tag|\phi F_3(r_1_L,r_2_L,TID_L)$

4）证明过程

当读写器收到消息 M_1，也即是 $Reader\lhd *(i)$，读写器查找后台数据库记录(i，ID，TIDi_L，TIDi_R，AckBit)，检索符合的标签标号信息 i，如果检索成功，读写器初次识别标签成功，也即是 $Reader|\equiv\phi(i)$，安全目标 D_1 得证。

当标签收到消息 M_2 后，也即是到 A=$TID_L\oplus r_1$、B=$TID_R\oplus r_2$，由初始化假设 H_5：$Tag|\equiv\#(r_1,r_2)$ 可知 $Tag|\equiv\#(r_1)$，再由初始化假设 H_1：$Tag\in(i,ID,TID_L,TID_R)$ 可知 $Tag\in(TID_L)$，$Tag|\equiv\phi(TID)\Rightarrow\phi(r_1,TID)$，再根据新鲜性规则 F1 可得 $Tag|\equiv\#(r_1,TID_L)$，继续根据新鲜性规则 F1，可得 $Tag|\equiv\#F_1(r_1,TID_L)$，接着根据消息解析规则 I1（其中，$Tag\in(i)$、$Tag|\equiv T\xleftrightarrow{i}R$、$Tag|\equiv\phi(r_1,TID)$、$Tag\lhd *(r_1)$、$Tag|\equiv\#F_1(r_1,TID_L)$），终得 $Tag|\equiv Reader|\sim\#F_1(r_1,TID_L)$，安全性目标 D_2 得证。安全目标 D_3：由初始化假设 H_5：$Tag|\equiv\#(r_1,r_2)$ 可知 $Tag|\equiv\#(r_2)$，再由初始化假设 H_1：$Tag\in(i,ID,TID_L,TID_R)$ 可知 $Tag\in(TID_R)$，再由可识别规则 R_1、R_2 可以得到 $Tag|\equiv\phi(TID)\Rightarrow\phi(r_2,TID)$，再根据新鲜性规则 F1 可得 $Tag|\equiv\#(r_2,TID_R)$，继续根据新鲜性规则 F1，可得 $Tag|\equiv\#F_2(r_2,TID_R)$，接着根据消息解析规则 I1（其中，$Tag\in(i)$、$Tag|\equiv Tag\xleftrightarrow{i}Reader$、

chinaXiv:201810.00031v1

$Tag\mid\equiv\phi(r_2,TID)$、$Tag\lhd*(r_2)$、$Tag\mid\equiv\#F_2(r_2,TID_R)$），可得 $Tag\mid\equiv Reader\mid\sim\#F_2(r_2,TID_R)$，安全性目标 D_3 得证。

当读写器收到来自标签的消息 M_3 后，也即是：$C=Rot(r_1_L,TID_L)\oplus Rot(r_2_L,TID_L)$，读写器再次查找后台数据库记录($i$，$ID$，$TID_i_L$，$TID_i_R$，$AckBit$)，以及随机数 r_1、r_2，验证标签，可以得到 $Reader\mid\equiv\phi(r_1_L,r_2_L,TID_L)$，最后再根据可识别规则 R1：得到 $Reader\mid\equiv\phi F(r_1_L,r_2_L,TID_L)$，预期目标 D_4 实现。

4　算法安全性分析

本章主要从第 2 章提到文献[5,8,9]中存在的标签匿名性、重放攻击、密钥伪造攻击三个方面对本文改进算法进行分析。

在三个应用场景下改进算法都可以保证标签匿名性，分析如下：因为在三种场景下标签收到读写器的请求后，并没有直接利用标签本身的 *ID* 信息进行计算，而是将标签的标号信息 i 进行初次识别，并且将标签 *ID* 信息进行加密得到假名 *TID*，$TID=Rot(ID_L,ID_R)$，再将 *TID* 分成左、右两部分，即使攻击者通过窃听得到<*A*、*B*、*C*>也无法轻易以第二节描述的解密方式得到 *TID* 以及随机数 r_1、r_2 结果，改进协议可以在三种场景下安全的保证标签匿名性，而根据本文第 2 章相关研究中表明文献[8]不能保证标签匿名性。

在三个应用场景下改进算法都可以抵抗重放攻击，分析如下：基于单标签和多标签的应用场景下，无论是攻击者窃听重放<*A*、*B*、*C*>中的任意消息（$A=TID_L\oplus r_1$、$B=TID_R\oplus r_2$、$C=Rot(r_1_L,TID_L)\oplus Rot(r_2_L,TID_L)$），都会因为随机数错误而使算法终止，在基于群组标签密钥生成场景中，改进算法在密钥 Key 的生成中加入随机数 *r*，$Key=Sac(ID_1,r)\oplus Sac(ID_2,r)\oplus\cdots\oplus Sac(ID_i,r)$，即使攻击者重放 A，因为攻击者不知道标签 (ID_i,TID_i_L,TID_i_R) 身份字段，也无法攻击成功，并且读写器端(i，ID，TID_i_L，TID_i_R，$AckBit$) *AckBit* 激活标志的存在，使得标签 *AckBit* 已经置 1，当攻击者重放消息时，*AckBit* 激活标志检验出错误，算法一样会终止。因此，改进协议可以在三种场景下安全的抵抗重放攻击，而根据本文第 2 节相关研究中表明文献[5，8，9]均不能抵抗重放攻击。

在三个应用场景下改进算法都可以抵抗密钥伪造攻击，分析如下：因为在基于单标签应用场景下改进算法共享密钥的加密方式是 $Key=Sac(r_1_R,ID)\oplus Sac(r_2_R,ID)$、基于多标签应用场景下改进算法共享密钥的加密方式是 $Key_i=Sac(r_1_R,ID_i)\oplus Sac(r_2_R,ID_i)$，可以看出这两种场景下生成密钥的方式都需要随机数和标签身份信息的加入，而攻击者在整个通信过程中都不曾得到标签 ID 的信息，只有假名 *TID* 的参与，攻击者并不能获得完整的数据；在基于群组标签应用场景下改进算法共享密钥的加密方式是 $Key=Sac(ID_1,r)\oplus Sac(ID_2,r)\oplus\cdots\oplus Sac(ID_i,r)$，而这第三种组密钥的产生方法中也同样引入随机数 r，标签必须计算出所有组内正确的解密关键因子 $Sac(ID_i,r)$，才可以顺利的破解组密钥 $Key=K_i\oplus Sac(ID_i,r)$，并且因为 *AckBit* 激活标志的存在，必须保证读写器对组内所有标签的记录都是(i，ID，TID_i_L，TID_i_R，$AckBit$=1)，读写器才会为标签生成统一的组密钥(i，ID，TID_i_L，TID_i_R，Key，$AckBit$=1)，因此，改进协议可以在三种场景下安全的抵抗密钥伪造攻击，而根据本文第 2 节相关研究中表明文献[5、8、9]均不能抵抗密钥伪造攻击。

5　改进算法性能分析

根据第 4 节算法形式化证明以及第 5 节安全性对比分析，下面给出相关文献与本文算法的安全性对比，见表 3，其中，√表示满足安全性；×表示不能满足安全性。

表 3　算法安全性对比

攻击类型	文献[5]	文献[8]	文献[9]	本算法
标签匿名	√	×	×	√
重放攻击	√	×	√	√
密钥伪造	×	×	×	√
算法证明	×	×	√	√

由于群组密钥组标签密钥无线生成场景和批量标签密钥无线生成场景下因为标签数量的不同无法计算对比，这里不再对比说明，本节主要统一对单个标签密钥场景下密钥无线生成算法，从标签的计算量、存储量和通信量三个方面与相关文献进行性能分析对比，如表 4 进行说明，在表 4 中，Xt 表示异或运算，PRNG 表示随机数产生器，R 表示移位运算，Rt 表示循环移位运算，Sa 表示自组合交叉位运算，假名 TID、标签唯一标志 ID、密钥 Key、随机数的长度都是 I，X 表示认证过程中的临时存储空间，通信量的单位为 L。

表 4　单个标签密钥生成改进算法性能对比

相关文献	计算量	存储空间	通信量
文献[5]	Xt+PRNG	I+X	L
文献[8]	7Xt	4I+X	L
文献[9]	5Xt+R	2I+X	L
本文	4Xt+2Rt+2Sa	3I+X	2L

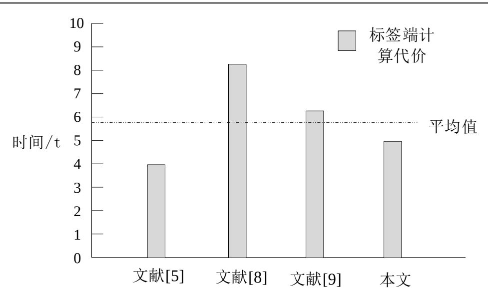


图 4　相关文献标签计算代价柱状对比图

通过表 3、4，图 4 可以看出，对于单个标签密钥生成算法，相较于文献[5，8，9]，本文算法无论是标签计算量、存储空间还是通信量和对比算法类似，达到超轻量标准，但是相较于对比算法，本文的改进算法在保证算法安全性更高的同时标签端计算代价并没有提高，标签端计算代价低于平均值，满足低成

ChinaXiv合作期刊
chinaXiv:201810.00031v1

本应用。

6　结束语

本文在 RFID 密钥无线生成三种场景下分别提出了更安全的改进算法，给出完整 GNY 逻辑证明过程，表明算法安全可行性，同时在满足 RFID 系统低成本应用的条件下弥补了原算法在标签匿名性、重放攻击、密钥伪造攻击三个安全方面的不足。

参考文献：

[1] Shen J, Tan H, Zhang Y, *et al.* A new lightweight RFID grouping authentication protocol for multiple tags in mobile environment [J]. Multimedia Tools & Applications, 2017: 1-23.

[2] 王金茹. 基于部分假名 ID 的 RFID 系统密钥无线生成算法 [J]. 计算机工程与应用, 2018, 54 (1): 128-132. (Wang Jinru. Wireless key generation algorithm for RFID system based on partial pseudonym ID [J]. Computer Engineering and Applications, 2018, 54 (1): 128-132)

[3] Chen H, Wang Z, Xia F, *et al.* Efficiently and Completely Identifying Missing Key Tags for Anonymous RFID Systems [J]. IEEE Internet of Things Journal, 2017, PP (99): 1-1.

[4] 张兵, 秦志光, 万国根. 基于 PKI 和 CPK 的 RFID 系统混合密钥管理机制研究 [J]. 电子科技大学学报, 2015, 44 (3): 415-421. (Zhang Bing Qin Zhiguang Wan Guogen. Study on Hybrid Key Management Mechanisms of RFID System Based on PKI and CPK [J]. Journal of University of Electronic Science and Technology of China, 2015, 44 (3): 415-421.)

[5] 鲁力 RFID 系统密钥无线生成 [J]. 计算机学报, 2015, 38 (4): 822-832. (Lu Li. Wireless Key Generation for RFID Systems [J]. Chinese Journal of Computers, 2015, 38 (4): 822-832.)

[6] 简碧园, 刘道微. 基于位运算的 RFID 系统密钥无线生成算法 [J]. 计算机工程与应用, 2017, 53 (16): 98-103. (Jian Biyuan Liu Daowei. Wireless key generation algorithm for RFID system based on bit operation [J]. Computer Engineering and Applications, 2017, 53 (16): 98-103.)

[7] 斯进, 简碧园, 刘道微. RFID 系统密钥无线生成算法 [J]. 计算机工程与设计, 2017, 38 (10): 2686-2690. (Si Jin Jian Biyuan Liu Daowei, Wireless key generation algorithm for RFID system [J]. Computer Engineering and Design, 2017, 38 (10): 2686-2690.)

[8] 黄琪, 凌捷, 何晓桃. 一种改进的基于标签部分 ID 的 RFID 密钥无线生成算法 [J]. 计算机科学, 2017, 44 (1): 172-175. (Huang Qi Ling Jie He Xiaotao. Improved RFID Key Wireless Generation Algorithm Based on Tag Part ID [J]. Computer Science, 2017, 44 (1): 172-175.)

[9] 苏庆, 李倩, 彭家进, 等. 基于假名标志的加密 RFID 系统无线密钥生成协议 [J]. 计算机工程, 2017, 43 (8): 173-177. (Su Qing Li Qian Peng Jiajin, etal. Wireless Key Generation Protocol for Encrypted RFID System Based on Pseudonym Logo [J]. Computer Engineering, 2017, 43 (8): 173-177.)

[10] 张朝晖, 刘悦, 刘道微. 基于标签 ID 的 RFID 系统密钥无线生成算法 [J]. 计算机应用研究, 2017, 34 (1): 261-263. (Zhang Zhaohui Liu Yue Liu Daowei. Based on tag's ID wireless key generation for RFID system algorithm [J]. Application Research of Computers, 2017, 34 (1): 261-263.)

[11] Labbi Z, Maarof A, Senhadji M, *et al.* Hybrid Encryption Approach Using Dynamic Key Generation and Symmetric Key Algorithm for RFID Systems [C]// Proc of International Conference on Networked Systems. Springer International Publishing, 2016: 244-249.

[12] Dimitriou T. Key evolving RFID systems: Forward//backward privacy and ownership transfer of RFID tags [J]. Ad Hoc Networks, 2016, 37: 195-208.

[13] 汪小威, 卢志翔, 陆涛. 基于自组合交叉位运算的超轻量移动认证协议 [J]. 计算机工程与设计, 2017 (12): 3252-3257. (Wang Xiaowei, Lu Zhixiang, Lu Tao. Ultra-lightweight mobile authentication protocol based on self-assembly crossover [J]. Computer Engineering and Design, 2017 (12): 3252-3257.)

[14] Garcia R, Modesti P. An IDE for the Design, Verification and Implementation of Security Protocols [C]// Proc of IEEE International Symposium on Software Reliability Engineering. Washington DC: IEEE Computer Society, 2017: 157-163

[15] 朱宏峰, 刘天华. 隐私保护安全协议研究 [M]. 北京: 科学出版社, 2015. (Zhu Hongfeng, Liu Tianhua. Research on privacy protection security protocol [M]. Beijing: Science Press, 2015.)